LYNCH CARPENTER, LLP
(Eddie) Jae K. Kim (SBN: 236805)
ekim@lcllp.com
Tiffine E. Malamphy (SBN 312239)
tiffine@lcllp.com
117 E Colorado Blvd, Ste 600
Pasadena, CA 91105-3712
Tel.: (213) 723-0707
Fax: (858) 313-1850

Attorneys for Plaintiff
and Proposed Class Counsel

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

CYNTHIA HAYS, on behalf of herself and all others similarly situated,

Plaintiff,

v.

LINKEDIN CORPORATION,

Defendant.

Case No.: 5:25-cv-4181

CLASS ACTION COMPLAINT

Plaintiff Cynthia Hays ("Plaintiff"), on behalf of herself and all others similarly situated, asserts that following against Defendant LinkedIn Corporation ("LinkedIn" or "Defendant"), based upon personal knowledge, where applicable, information and belief, and the investigation of counsel:

NATURE OF THE ACTION

1. Plaintiff brings this case to address Defendant's unlawful practice of intercepting Plaintiff's and Class Members' confidential personal health communications with Covered California, without their knowledge or consent.

2. LinkedIn is a social networking site that is predominately used for professional networking and career development.

3. Like other social networking platforms—such as Facebook, Snapchat, and TikTok—LinkedIn offers website operators, such as Covered California, a tracking technology that can be embedded on a website to collect and analyze how individuals interact with a given website.

4. LinkedIn's tracking technology—the LinkedIn Insight Tag ("Insight Tag")—is a snippet of JavaScript computer code embedded on a third-party website that tracks a visitor's actions as they navigate through the website. It logs the URLs of pages they visit, the buttons they click, their IP address, and more.[1] This information is collected in real time and sent to LinkedIn who then utilizes the harvested data to target individuals with advertisements on its social media platform.

5. LinkedIn profits from this large-scale data collection. The Insight Tag is marketed towards businesses that use LinkedIn Ads as a way to "optimize" their advertising campaigns and LinkedIn generates substantial revenue through its advertising services.[2]

6. These benefits appeal to website operators, with over 150,000 websites in the United States utilizing the Insight Tag.[3]

7. Recently, it was discovered that the Insight Tag was embedded on Covered California's website, https://www.coveredca.com/, the organization that lets Californians shop for health insurance under the Affordable Care Act.[4]

8. When a visitor to https://www.coveredca.com/ shopped for health insurance, the Insight Tag intercepted sensitive health information, and sent that information to LinkedIn, providing Defendant with intimate personal facts and data in the form of their sensitive health information.

9. The intercepted data included information from forms website visitors filled out, including sensitive health information such as whether they were blind, pregnant, or used prescription medication; along with information about visitor's ethnicity or marital status. The Insight Tag also captured information about visitors' doctors and specialties if they selected doctors covered by a specific health plan offered through Covered California.[5]

---

[1] *Insight Tag*, LinkedIn, https://business.linkedin.com/marketing-solutions/insight-tag (last accessed May 15, 2025).

[2] *Id.*, *see also* Nicola Agius, *LinkedIn Ad Prices Surge as Advertisers' X Boycott Continues*, SEARCH ENGINE LAND (Jan. 2, 2024), https://searchengineland.com/linkedin-ad-prices-climb-advertisers-boycott-x-436152.

[3] *LinkedIn Insights Usage Statistics*, BuiltWith, https://trends.builtwith.com/analytics/LinkedIn-Insights (last accessed May 15, 2025).

[4] Tomas Apodaca and Colin Lecher, *How California Sent Residents' Personal Health Data to LinkedIn*, THE MARKUP (April 28, 2025), https://themarkup.org/pixel-hunt/2025/04/28/how-california-sent-residents-personal-health-data-to-linkedin.

[5] *Id.*

10. LinkedIn thereafter monetized the harvested sensitive health information received though the Insight Tag by utilizing it to generate highly profitable targeted advertising; the type of advertising on which it relies for a substantial portion of its revenue.

11. The targeted advertising LinkedIn offers for sale includes the ability to target individuals based on specific sensitive health information that a visitor has provided to Covered California.

12. LinkedIn's actions constitute an extreme invasion of Plaintiff's and Class members' right to privacy and violate federal and state statutory and common law.

PARTIES

13. Plaintiff Cynthia Hays is an adult and citizen of California where she intends to remain.

14. Defendant LinkedIn Corporation is a corporation organized under the laws of Delaware with its primary place of business located at 1000 W. Maude Ave, Sunnyvale, California 94085.

JURISDICTION & VENUE

15. This Court has federal question subject matter jurisdiction under 28 U.S.C. § 1331 because this suit is brought under the laws of the United States (18 U.S.C. §§ 2510, *et seq.*).

16. This Court has supplemental jurisdiction over the remaining state law claims pursuant to 28 U.S.C. § 1367 because the state law claims form part of the same case or controversy under Article III of the United States Constitution.

17. This Court has personal jurisdiction over Defendant because its principal place of business is in this District and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

18. Venue is proper under 18 U.S.C § 1391(b)(1) because Defendant's principal place of business is in this District.

FACTUAL BACKGROUND

19. Covered California is California's health insurance marketplace that was established under the Affordable Care Act to help Californian's find and afford health insurance plans. Over 1.9 million individuals have enrolled in health insurance through Covered California.[6]

20. Covered California operates the website and subpages of coveredca.com, which allows Californias to shop for and compare health insurance plans.

21. Unbeknownst to Californians shopping for health insurance on coveredca.com, however, the Insight Tag was embedded on coveredca.com and its subpages, collecting information Californians submitted to Covered California.

22. Indeed, a recent investigation by The Markup revealed that between February 2024 and April 2025, the Insight Tag was tracking visitors coveredca.com and disclosing their health information submitted to Covered California to LinkedIn.[7]

A. How LinkedIn's Insight Tags Work

23. Web browsers are software applications that allow consumers to navigate the internet and view and exchange electronic information and communications. Each "client device" (such as computer, tablet, or smart phone) accessed web content through a web browser (*e.g.*, Google's Chrome browser, Mozilla's Firefox browser, Apple's Safari browser, and Microsoft's Edge browser).

24. Every website is hosted by a computer "server" that holds the website's contents and through which the website owner exchanges files or communications with Internet users' client devices via their web browsers.

25. Web communications consist of HTTP or HTTPS Requests and HTTP or HTTPS Responses. Any given browsing session may consist of thousands of individual HTTP Requests and HTTP Responses, along with corresponding cookies:

[6] *Covered California Reaches Record-Breaking 1.9M Enrollees Before Open Enrollment's Jan. 31 Deadline*, Covered California, https://www.coveredca.com/newsroom/news-releases/2025/01/29/covered-california-reaches-record-breaking-1-9m-enrollees-before-open-enrollment-s-jan-31-deadline/ (last accessed May 15, 2025).

[7] Apodaca, *supra* n. 4.

- HTTP Request: an electronic communication sent from the client device's browser to the website's server. GET Requests are one of the most common types of HTTP Requests. In addition to specifying a particular URL (*i.e.*, web address), GET Requests can also send data to the host server embedded inside the URL, and can include cookies. POST Requests are a separate type of HTTP Request that can send a large amount of data outside of the URL (*e.g.*, uploading a PDF to a court's ECF system for filing a motion).
- Cookies: a small text file that can be used to store information on the client device which can later be communicated to a server or servers. Cookies that have been placed on the client device are sent with HTTP Requests from client devices to the host server. Some cookies are "third-party cookies" which means they can store and communicate data to the cookie owner's website when the user is visiting an entirely different website.
- HTTP Response: an electronic communication that is sent as a reply to the client device's web browser from the host server in response to an HTTP Request. HTTP Responses may consist of a web page, another kind of file, text information, or error codes, among other data. HTTP Responses can also send cookies or other code hidden and embedded in the webpage to the client device's browser.

26. When an individual visits Covered California's website, an HTTP Request is sent from that individual's web browser to Covered California's servers that asks the website to retrieve certain information. The HTTP Response from Covered California's servers sends the requested information in the form of "Markup." This is the foundation for the pages, images, words, buttons, and other features that appear on the visitor's screen as they navigate the website.

27. Every website is comprised of Markup and "Source Code." Source Code is simply a set of instructions that commands the website visitor's browser to take certain actions when the web page first loads or when a specified event triggers the code.

28. Source code may also command a web browser to send data transmissions to third parties in the form of HTTP Requests quietly executed in the background without notifying the web browser's user. Defendant's Insight Tag is source code that does just that, and acts much like a traditional wiretap. When members visit Covered California website via an HTTP Request to Covered California's server,

Covered California's server sends an HTTP Response including the Markup that displays the Webpage visible to the user along with Source Code that includes Defendant's Insight Tags. Once the Webpage loads in the members browser, Defendant's Insight Tags quietly wait for a communication from the member to trigger the tag, which intercepts those communications intended only for Covered California and delivers the content of those communications to Defendant.

29. Insight Tags manipulate the web users' browser by secretly instructing it to duplicate the members' communications (HTTP Requests) with Covered California and to send those communications to LinkedIn. These transmissions occur contemporaneously, invisibly, and without the user's knowledge.

30. The Insight Tags are programmed to automatically track and transmit communications made between Covered California and its users. The Insight Tags execute instructions that effectively open a hidden spying window into the patient's browser through which LinkedIn can intercept the visitor's data, actions, and communications with Covered California.

31. The user visiting Covered California only sees the Markup, not Defendant's Insight Tags or the underlying HTTP Requests and Responses.

32. The inclusion of Insight Tags on a website does not provide any substantive content to the website user. In other words, LinkedIn does not provide anything to the user, but only serves to track user data and communications to further the marketing purposes of the website owner (*i.e.*, to bolster profits).

33. Thus, without any knowledge, authorization, or action by a user, LinkedIn uses its Insight Tag source code to commandeer the computing devices of Covered California users, causing the device's web browser to contemporaneously and invisibly re-direct communications to LinkedIn.

34. In this case, LinkedIn intercepted Plaintiff's and Class Members' Personal Health Information to acquire data to power its targeted advertising business.

35. Consequently, when Plaintiff and Class Members visit Covered California and communicated their Personal Health Information, including, but not limited to, precise text of search queries about specific doctors and prescription drugs; users' downloads of information about specific

illnesses, conditions, and mental health disorders; summaries of communications between patients and Covered California; these communications are simultaneously intercepted and transmitted to LinkedIn.

36. LinkedIn tracks internet users with IP addresses, cookies, geolocation, and other unique device identifiers.

37. LinkedIn also uses personally identifiable cookies, such as "li_at" and "li_rm," which contain digitally signed and encrypted records of a user's LinkedIn account.

38. LinkedIn uses cookies like li_at and li_rm to help customize ads on LinkedIn. For example, LinkedIn uses such cookies to remember users' most recent searches, previous interactions with an advertiser's ads or search results, and visits to an advertiser's website. This helps LinkedIn show customized ads to users on LinkedIn.

39. LinkedIn cookies thus provide personally identifiable data about patients who visit Covered California's website, and LinkedIn intercepts this information for its targeted advertising purposes.

B. LinkedIn Was Well Aware that the Intercepted Data Included Sensitive Health Information.

40. LinkedIn was well-aware that providing its Insight Tag to Covered California, the embedded Insight Tag would intercept and disclose to LinkedIn, Plaintiff's and Class Members' sensitive health information.

41. By the design of Insight Tag, *i.e.*, sending all interactions on a website to LinkedIn, Defendant was keenly aware that the Insight Tag would intercept individuals' sensitive health information when embedded on websites such as that of Covered California.

42. Indeed, LinkedIn knew it was receiving sensitive health information through the Insight Tag enabled on Covered California's website given the well-reported issues related the use of tracking technologies on websites involving sensitive health information.

43. For instance, in 2021, the FTC reached a settlement with Flo Health, Inc., arising from allegations that the fertility-tracking app was sharing sensitive health information from millions of its users with marketing and analytics firms, including Meta and Google.[8]

44. Further, in 2022, investigations from The Markup revealed that hospitals across the country were sharing individuals' health information with Meta via its own tracking technology known as the Meta Pixel.[9]

45. Since then, the Federal Trade Commission has engaged in numerous enforcement actions against companies, including online pharmacy GoodRx and telehealth companies such as Monument for sharing users' health information to Meta and Google without individuals' consent.[10]

C. Plaintiff Had Her Sensitive Health Information Intercepted by LinkedIn

46. Plaintiff fell victim to LinkedIn's unlawful interception of her sensitive health information when utilizing Covered California's website.

47. While the Insight Tag was embedded on Covered California's website, Plaintiff visited Covered California's website and related subpages to shop for health insurance through California's health insurance exchange.

48. When shopping for health insurance through Covered California, Plaintiff filled out forms and provided sensitive health information to Covered California.

49. Unbeknownst to Plaintiff, however, Covered California had installed the Insight Tag on the website. This resulted in the interception of Plaintiff's sensitive health information by LinkedIn without her consent.

---

[8] *FTC Finalizes Order with Flo Health, a Fertility-Tracking App that Shared Sensitive Health Data with Facebook, Google, and Others,* FTC (June 22, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared-sensitive-health-data-facebook-google.

[9] Todd Feathers et al., *Facebook Is Receiving Sensitive Medical Information from Hospital Websites*, THE MARKUP (June 16, 2022), https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites.

[10] Katie Palmer, *FTC Cracks Down on Telehealth Addiction Service Monument for Sharing Health Data*, THE MARKUP (April 19, 2024), https://themarkup.org/pixel-hunt/2024/04/19/ftc-cracks-down-on-telehealth-addiction-service-monument-for-sharing-health-data.

50. After using the Covered California website, Plaintiff began receiving targeted advertising on her LinkedIn account that was directly related to her interactions on Covered California's website and information she provided when shopping for health insurance coverage.

51. Plaintiff never consented to the interception of her sensitive health information by LinkedIn.

52. Plaintiff reasonably believed that her interactions with Covered California were private and would be intercepted by a third-party, let alone utilized for advertising purposes.

53. Plaintiff was dismayed and outraged when she learned that LinkedIn had been capturing her sensitive health information for advertising purposes without her consent.

D. Defendant's Interception Occurred Without Plaintiff's or Class Members' Knowledge or Consent

54. Plaintiff and Class members have no idea LinkedIn collects and uses their sensitive health information when they interacted with Covered California's website because the Insight Tag runs only in the background of the website.

55. For instance, when Plaintiff was on Covered California's website, there was no indication that the Insight Tag was embedded or that it would collect her sensitive health information.

56. Covered California's "Privacy Policy" states that "it strictly limits personal information it collects to that which is both relevant and necessary to fulfill the functions required of us under the Affordable Care Act and applicable California state law" and that California Covered only used Plaintiff's and Class Members' information for: (1) determining eligibility for health care coverage; (2) facilitating initial enrollment in health coverage; (3) managing your enrollment in health coverage; (4) complying with federal or state law; and (5) performing other required exchange functions.[11]

57. Covered California's Privacy Policy further states that "Covered California will only share your personal information with government agencies, qualified health plans or contractors which

[11] *Privacy Policy*, Covered California (effective Oct. 6, 2020), *available at* https://www.coveredca.com/pdfs/privacy/CC_Privacy_Policy.pdf (last accessed May 15, 2025).

help to fulfill a required Exchange function." At no time does the Privacy Policy disclose that individuals' sensitive health information will be disclosed to LinkedIn.[12]

58. The collection of Plaintiff's and Class members' sensitive health information is also inconsistent with LinkedIn's Advertising polices Data Policy. LinkedIn requires those advertising on its platform to "comply[ ] with applicable privacy and data protection laws and regulations" and to not "use tracking cookies to track users across sites without full disclosure and consent of the users."[13]

59. LinkedIn's Ads Agreement similarly requires those advertising on its platform to have "obtained valid consent (to the extent required by Applicable Law) from, the applicable individuals regarding any collection, transfer and use of their Audience Data for Matched Audiences and Analytics and the underlying technologies that enables these services."[14]

60. Neither Plaintiff nor Class Members knowingly consented to LinkedIn's interception of their sensitive health information when shopping for insurance on Covered California's website.

61. Accordingly, Defendant lacked authorization to intercept or use Plaintiff's and Class Members' sensitive health information.

E. Plaintiff and Class Members Have a Reasonable Expectation of Privacy in Their Sensitive Health Information

62. Plaintiff and Class Members have a reasonable expectation of privacy in their information communicated to Covered California, including their personal health information. Specifically, Plaintiff and Class Members had a reasonable expectation that while shopping for health insurance, their sensitive health information would not be intercepted by third parties, such as LinkedIn without, express authorization.

63. As one expert put LinkedIn's surreptitious collection of Plaintiff's and Class Members' sensitive health information is "'concerning and invasive' for a health insurance website to be sending

---

[12] *Id.*

[13] *LinkedIn Advertising Policy*, LinkedIn (revised Dec. 16, 2024), *available at* https://www.linkedin.com/legal/ads-policy (last accessed May 15, 2025).

[14] *LinkedIn Ads Agreement*, LinkedIn (updated Jan. 6, 2025), *available at* https://www.linkedin.com/legal/sas-terms (last accessed May 15, 2025).

data that was 'wholly irrelevant' to the uses of a for-profit company like LinkedIn." The expert further explained that "people don't expect that their health information will be collected and used in this way" and that "[t]his absolutely contradicts the expectation of the average consumer[.]"[15]

64. Indeed, multiple studies examining the collection and disclosure of consumers' sensitive medical information confirm that the disclosure of sensitive medical information violates expectations of privacy that have been established as general social norms. Empirical evidence demonstrates that "[w]hen asked, the overwhelming majority of Americans express concern about the privacy of their medical records." Sharona Hoffman & Andy Podgurski, *E-Health Hazards: Provider Liability and Electronic Health Record Systems*, 24 Berkley Tech L.J. 1523, 1557 (2009).

65. Privacy polls and studies also uniformly show that the overwhelming majority of Americans consider one of the most important privacy rights to be the need for an individual's affirmative consent before a company collects and shares its customers' data.

66. For example, a recent study by *Consumer Reports* showed that 92% of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing consumers' data, and the same percentage believed that internet companies and websites should be required to provide consumers with a complete list of the data that has been collected about them.[16]

67. Users act consistently with these preferences. For example, following a new rollout of the iPhone operating software—which asks users for clear, affirmative consent before allowing companies to track users—85 percent of worldwide users and 94 percent of U.S. users chose not to share data when prompted.[17]

68. These concerns are not hypothetical. For example, in 2021, the FTC brought charges against Flo Health, a company who, despite its express privacy claims, took control of users' sensitive

[15] Apodaca, *supra* n. 4.
[16] *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*, CONSUMER REPORTS (May 11, 2017), https://www.consumerreports.org/consumer-reports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety-a3980496907.
[17] Margaret Taylor, *How Apple screwed Facebook*, WIRED (May 19, 2021), https://www.wired.com/story/apple-ios14-facebook.

fertility data and shared it with third parties—a broken promise that, as the FTC described it, "left consumers feeling 'outraged, victimized, and violated.'"[18]

69. The concern about sharing personal medical information is compounded by the reality that advertisers view this type of information as particularly valuable. Indeed, having access to the data women share with their healthcare providers allows advertisers to obtain data on children before they are even born. As one recent article noted, "What is particularly worrying about this process of datafication of children is that companies . . . are harnessing and collecting multiple typologies of children's data and have the potential to store a plurality of data traces under unique ID profiles."[19]

70. Many privacy law experts have expressed serious concerns about individuals' sensitive medical information being disclosed to third-party companies like LinkedIn. As those critics have pointed out, having an individual's personal health information disseminated in ways the individual is unaware of could have serious repercussions, including affecting their ability to obtain life insurance, how much they might pay for such coverage, the rates they might be charged on loans, and the likelihood of their being discriminated against.

71. LinkedIn surreptitious interception and collection of sensitive health information therefore violated Plaintiff and Class Member's privacy interests.

F. Plaintiff's Personal Health Information Has Economic Value and Defendant's Interception Has Caused Economic Harm

72. It is common knowledge that there is an economic market for consumers' personal data—including the kind of data that LinkedIn has collected and disclosed from Plaintiff and Class Members.

73. In 2013, the *Financial Times* reported that the data-broker industry profits from the trade of thousands of details about individuals, and that within that context, "age, gender and location information" were being sold for approximately "$0.50 per 1,000 people."[20]

---

[18] Complaint, *In re Flo Health, Inc.* FTC File No. 1923133, Dkt. No. C-4747, https://www.ftc.gov/system/files/documents/cases/flo_health_complaint.pdf (last accessed May 15, 2025).

[19] Veronica Barassi, *Tech Companies Are Profiling Us From Before Birth*, THE MIT PRESS READER (Jan. 17, 2021), https://thereader.mitpress.mit.edu/tech-companies-are-profiling-us-from-before-birth.

[20] Emily Steel, *et al*, *How much is your personal data worth?*, FINANCIAL TIMES (updated Jul. 15, 2017), https://ig.ft.com/how-much-is-your-personal-data-worth.

74. In 2015, *TechCrunch* reported that "to obtain a list containing the names of individuals suffering from a particular disease," a market participant would have to spend about "$0.30" per name.[21] That same article noted that "Data has become a strategic asset that allows companies to acquire or maintain a competitive edge" and that the value of a single user's data can vary from $15 to more than $40 per user.[22]

75. Despite the protections afforded by law, there is an active market for health information. Medical information obtained from health providers garners substantial value because of the fact that it is not generally available to third party data marketing companies because of the strict restrictions on disclosure of such information by state laws and provider standards, including the Hippocratic oath. Even with these restrictions, however, a multi-billion-dollar market exists for the sale and purchase of such private medical information.[23]

76. Further demonstrating the financial value of Class Members' medical data, CNBC has reported that hospital executives have received a growing number of bids for user data.[24]

77. Further, individuals can sell or monetize their own data if they so choose. For example, Facebook has offered to pay individuals for their voice recordings,[25] and has paid teenagers and adults up to $20 a month plus referral fees to install an app that allows Facebook to collect data on how individuals use their smart phones.[26] A myriad of other companies and apps such as DataCoup, Nielsen

---

[21] Pauline Glikman and Nicolas Glady, *What's the Value of Your Data?*, TECHCRUNCH (Oct. 13, 2015), https://techcrunch.com/2015/10/13/whats-the-value-of-your-data.

[22] *Id.*

[23] Aaron Sankin, *Your medical data is for sale, and there's noting you can do about it*, REVEAL NEWS (Jan. 20, 2017), https://revealnews.org/blog/your-medical-data-is-for-sale-and-theres-nothing-you-can-do-about-it; *see also* Justin Sherman, *Your Health Data Might Be for Sale*, SLATE (Jun. 20, 2022), https://slate.com/technology/2022/06/health-data-brokers-privacy.html.

[24] Christina Farr, *Hospital execs say they are getting flooded with requests for your health data*, CNBC (Dec. 18, 2019), https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html.

[25] Jay Peters, *Facebook will now pay your for your voice recordings*, The Verge (Feb. 20, 2020), https://www.theverge.com/2020/2/20/21145584/facebook-pay-record-voice-speech-recognition-viewpoints-prounnciations-app.

[26] Saheli Roy Choudhury and Ryan Browne, *Facebook pays teens to install an app that could collect all kinds of data*, CNBC (Jan. 30, 2019), https://www.cnbc.com/2019/01/29/facebook-paying-users-to-install-app-to-collect-data-techcrunch.html.

Computer, Killi, and UpVoice also offer consumers money in exchange for access to their personal data.[27]

78. Given the monetary value that data companies have already paid for personal information in the past, LinkedIn has deprived Plaintiff and the Class Members of the economic value of their sensitive medical information by intercepting, collecting, and using, that information without consideration for Plaintiff's and the Class Member's property.

CLASS ACTION ALLEGATIONS

79. Plaintiff brings this action on behalf of herself and on behalf of all other persons similarly situated pursuant to Rule 23 of the Federal Rules of Civil Procedure.

80. Plaintiff seeks class certification for the following proposed Class:

> During the fullest period allowed by law, all persons in California who exchanged communications at the Covered California website (https://www.coveredca.com) or any of its subpages, while the Insight Tag operated on the Covered California website and its subpages.

81. Excluded from the proposed Class are: (1) any Judge or Magistrate presiding over this action and members of their families; (2) LinkedIn, LinkedIn's subsidiaries, affiliates, parents, successors, predecessors, and any entity in which the LinkedIn or their parents have a controlling interest and their current or former employees, officers, and directors; and (3) Plaintiff's counsel and LinkedIn's counsel.

82. Plaintiff reserves the right to redefine the Class and/or add Subclasses at, or prior to, the class certification stage, in response to discovery, or pursuant to instruction by the Court.

83. **Numerosity:** Fed R. Civ. P. 23(a)(1). The Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are millions of individuals whose Personal Health Information may have been improperly disclosed to third parties, and the Class is identifiable within Defendant's records.

[27] *See, e.g.,* Sam Hawrylack, *Apps that Pay You for Data Collection*, CreditDonkey (June 12, 2021), https://www.creditdonkey.com/best-apps-data-collection.html; *see also* Illia Lahunou, *Can You Earn Money From Your Data?*, Monetha Blog (April 28, 2022), https://www.monetha.io/blog/rewards/earn-money-from-your-data.

84. **Commonality and Predominance:** Fed. R. Civ. P. 23(a)(2) and (b)(3). There are questions of law and fact common to Plaintiff and Class Members which predominate over any questions affecting only individual members. A class action will generate common answers to the questions below, which are apt to drive resolution:

a. Whether the tracking technology used by LinkedIn is designed to send individually identifiable information from Defendant to third parties;

b. Whether LinkedIn intercepted and/or transmitted to third parties the contents of electronic communications between Covered California and its users without Plaintiff's and Class Members' consent;

c. Whether LinkedIn's interception of the contents of electronic communications between Covered California and its users occurred contemporaneous to their making;

d. Whether LinkedIn violated Plaintiff's and Class Members' privacy rights;

e. Whether LinkedIn's acts and practices were intentional;

f. Whether LinkedIn's acts and practices were negligent;

g. Whether LinkedIn profited from obtaining Plaintiff's and Class Members' personal health information;

h. Whether LinkedIn was unjustly enriched;

i. Whether LinkedIn's acts and practices harmed and continue to harm Plaintiff and Class Members and, if so, the extent of that injury;

j. Whether Plaintiff and Class Members are entitled to equitable relief including, but not limited to, injunctive relief, restitution, and disgorgement; and

k. Whether Plaintiff and Class Members are entitled to actual, statutory, punitive or other forms of damages, and other monetary relief.

85. These common questions of law and fact predominate over any questions affecting only the individual Class Members.

86. LinkedIn engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff individually and on behalf of the other Class Members. Identical statutory

and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quantity and quality, to the numerous questions that dominate this action.

87. **Typicality:** Fed. R. Civ. P. 23(a)(3). Plaintiff's claims are typical of those of other Class Members because all had their Personal Health Information compromised as a result of Defendant's interception of their electronic communications with Covered California. Plaintiff has no interests that are antagonist to, or in conflict with, the interests of other members of the Class. Plaintiff's claims arise out of the same set of facts and conduct as all other Class Members. Plaintiff and all Class Members are users of Covered California who transmitted information to Covered California and are victims of LinkedIn's conduct. All claims of Plaintiff and Class Members are based on LinkedIn's wrongful conduct and unauthorized interception of their communications.

88. **Adequacy of Representation:** Fed. R. Civ. P. 23(a)(4). Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiff has suffered are typical of other Class Members. Plaintiff has also retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

89. **Superiority:** Fed. R. Civ. P. 23(b)(3). Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against a large corporation like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

CAUSES OF ACTION

COUNT I
Violations Of Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2511(1) *Et Seq*. Unauthorized Interception, Use, And Disclosure (On Behalf of Plaintiff and the Class)

90. Plaintiff realleges and incorporates by reference paragraphs 1-89 as if fully set forth herein.

91. Plaintiff brings this claim on behalf of herself and all members of the Class.

92. The ECPA prohibits the intentional interception of the content of any electronic communication. 18 U.S.C. § 2511.

93. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed, or intentionally used in violation of the ECPA.

94. The ECPA protects both sending and receipt of communications.

95. **Electronic Communications**. The transmission of Personal Health Information between Plaintiff and Class Members and Covered California via its Website are "transfer[s] of signs, signals, writing,…data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate commerce" and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(12).

96. **Content**. The ECPA defines content, when used with respect to electronic communications, to "include[] any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8). The contents of Plaintiff's and Class Members' communications include, but are not limited to, IP addresses, LinkedIn cookies containing user account information, URLs, file downloads, and the text of search queries, all of which concern substance and meaning of Plaintiff's and Class Members' personal identities and protected health information such as medical conditions, prescriptions, and treatment.

97. **Interception**. The ECPA defines the interception as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device" and "contents … include any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(4), (8). Whenever Plaintiff and Class Members interacted with

Covered California, Defendant, through its Insight Tag source code, contemporaneously and intentionally acquired the contents of Plaintiff's and Class Members' electronic communications while those communications were in transmission, to persons or entities other than an addressee or intended recipient of such communication, *i.e.*, Covered California.

98. **Electronic, Mechanical, or Other Device**. The ECPA defines "electronic, mechanical, or other device" as "any device … which can be used to intercept a[n] … electronic communication[.]" 18 U.S.C. § 2510(5). The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

a. Plaintiff's and Class Members' browsers;

b. Plaintiff's and Class Members' computing devices;

c. Defendant's web-servers; and

d. The Insight Tag deployed by Defendant to effectuate the sending and acquisition of patient communications.

99. Whenever Plaintiff and Class Members interacted with Covered California, Defendant, through the Insight Tag source code, contemporaneously and intentionally used, and endeavored to use the contents of Plaintiff's and Class Members' electronic communications, for purposes other than providing health insurance services to Plaintiff and Class Members without authorization or consent, and knowing or having reason to know that the electronic communications were obtained in violation of the ECPA. 18 U.S.C. § 2511(1)(d).

100. By intentionally disclosing or endeavoring to disclose the electronic communications of Plaintiff and Class Members to affiliates and other third parties, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(c).

101. By intentionally using, or endeavoring to use, the contents of the electronic communications of Plaintiff and Class Members, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(d).

102. Defendant intentionally used the intercepted communications to increase its profit margins. Defendant specifically used Insight Tags to track and utilize Plaintiff's and Class Members' Personal Health Information for financial gain.

103. Defendant was not acting under color of law to intercept Plaintiff's and Class Members' wire or electronic communication.

104. Plaintiff and Class Members did not authorize LinkedIn to acquire the content of their communications for purposes of invading Plaintiff's privacy.

105. Any purported consent that Defendant received from Plaintiff and Class Members was not valid.

106. The ECPA provides that a "party to the communication" may liable where a "communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State." 18 U.S.C § 2511(2)(d).

107. Defendant intentionally intercepted the contents of Plaintiff's and Class Members' electronic communications for the purpose of committing a tortious or criminal act in violation of the Constitution or laws of the United States or of any State—namely, invasion of privacy, among others.

108. Plaintiff and Class Members have suffered damages as a direct and proximate result of Defendant's invasion of privacy in that:

a. Learning that Defendant has intruded upon, intercepted, transmitted, shared, and used their individually-identifiable health information (including information about their medical symptoms, conditions, and concerns, medical appointments, healthcare providers and locations, medications and treatments, and health insurance and medical bills) for commercial purposes has caused Plaintiff and the Class Members to suffer emotional distress;

b. Defendant received substantial financial benefits from its use of Plaintiff's and Class Members' individually-identifiable patient health information without providing any value or benefit to Plaintiff or the Class Members;

c. Defendant received substantial, quantifiable value from its use of Plaintiff's and Class Members' individually-identifiable health information, such as building informational

profiles of users and determining what ads people see on its website, without providing any value or benefit to Plaintiff or the Class Members; and

d. The diminution in value of Plaintiff's and Class Members' PII and PHI and the loss of privacy due to Defendant making sensitive and confidential information, such as medical conditions and treatments that Plaintiff and Class Members intended to remain private no longer private.

109. As a result of Defendant's violation of the ECPA, Plaintiff and Class Members entitled to all damages available under 18 U.S.C. § 2520, including statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000, equitable or declaratory relief, compensatory and punitive damages, and attorney's fees and costs.

COUNT II
Common Law Invasion of Privacy – Intrusion Upon Seclusion
(On Behalf of Plaintiff and the Class)

110. Plaintiff realleges and incorporates by reference paragraphs 1-109 as if fully set forth herein.

111. Plaintiff brings this claim on behalf of herself and on behalf of the Class.

112. California common law recognizes a cause of action for intrusion upon seclusion.

113. The Personal Health Information of Plaintiff and Class Members consists of private and confidential facts and information that were never intended to be shared beyond private communications.

114. Plaintiff and Class Members had a reasonable expectation of privacy in their sensitive health information.

115. LinkedIn intentionally intruded upon Plaintiff's and Class Members' private life, solitude, or seclusion by intercepting the contents of their communications with Covered California.

116. Plaintiff and Class Members did not consent to, authorize, or know about LinkedIn's intrusion at the time it occurred. Plaintiff and Class Members never agreed that LinkedIn could intercept the sensitive health information they shared with Covered California.

117. Plaintiff and Class Members had an interest in precluding the dissemination and/or misuse of their information and communications and in conducting their personal activities without

intrusion or interference, including the right to not have their personal information intercepted and utilized for business gain.

118. LinkedIn's conduct is highly objectionable to a reasonable person and constitutes an egregious breach of the social norms underlying the right to privacy because Plaintiff's and Class Members' sensitive health information is private and was intended to remain private and confidential.

119. Plaintiff and Class members were harmed by LinkedIn's wrongful conduct as that conduct has caused Plaintiff and the Class mental anguish and suffering arising from their loss of privacy and confidentiality of their sensitive health information.

120. As a direct and proximate result of LinkedIn's conduct, Plaintiff and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

COUNT III
Violation of California Constitution, Art. I § 1 – Invasion of Privacy
(On behalf of Plaintiff and the Class)

121. Plaintiff realleges and incorporates by reference paragraphs 1-120 as if fully set forth herein.

122. Plaintiff brings this claim on behalf of herself and on behalf of the Class.

123. Article I, Section 1 of the California Constitution states "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy."

124. Plaintiff and Class Members had, and continue to have, a legally protected interest in their sensitive medical and personal information that they provided to Covered California, deriving from common law and state and federal statutes, including, *inter alia*, HIPAA, The California Invasion of Privacy Act, and The Confidentiality of Medical Information Act.

125. Plaintiff and members of the Class had a reasonable expectation of privacy in their sensitive medical information and personal data, because Plaintiff and members of the Class did not consent to LinkedIn intercepting their communications and acquiring their sensitive information and personal data.

126. LinkedIn intentionally collected and shared Plaintiff's and Class Members' sensitive medical and personal information without their consent.

127. LinkedIn's conduct is highly objectionable to a reasonable person and constitutes an egregious breach of the social norms underlying the right to privacy because Plaintiff's and Class Members' sensitive health information is private and was intended to remain private and confidential.

128. Plaintiff and Class Members were harmed by LinkedIn's wrongful conduct, which has caused Plaintiff and the Class mental anguish and suffering arising from their loss of privacy and confidentiality of their sensitive health information.

129. As a direct and proximate result of LinkedIn's conduct, Plaintiff and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

COUNT IV
Violation of the California Invasion of Privacy Act ("CIPA")
Cal. Penal Code §§ 630, et seq.
(on Behalf of Plaintiff and the Class)

130. Plaintiff realleges and incorporates by reference paragraphs 1-129 as if fully set forth herein. Plaintiff brings this claim on behalf of herself and on behalf of the Class.

131. To establish liability under Section 631(a) of the CIPA, a plaintiff must establish that the defendant, "by means of any machine, instrument, contrivance, or in any other manner" either (1) "[i]ntentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system;" (2) "[w]illfully and without the consent of all parties to the communication, or in any unauthorized manner, reads or attempts to read or learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line or cable or is being sent from or received at any place within this state;" (3) "[u]ses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained;" or (4) "[a]ids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section."

132. Section 631(a) applies to internet communications and thus applies to Plaintiff's and the Class's sensitive health information which was intercepted by Defendant through the Insight Tag. *See Javier v. Assurance IQ, LLC*, No. 21-16351, 2022 WL 1744107, at *1 (9th Cir. May 31, 2022) (citing Cal. Penal Code § 631(a) ("Though written in terms of wiretapping, Section 631(a) applies to Internet communications. It makes liable anyone who 'reads, or attempts to read, or to learn the contents' of a communication 'without the consent of all parties to the communication.'"); *In re Facebook, Inc. Internet Tracking Litig*., 956 F.3d 589, 608 (9th Cir. 2020) (reversing dismissal of CIPA and common law privacy claims based on Facebook's collection of consumers' Internet browsing history).

133. LinkedIn's Insight Tags are a "machine, instrument, contrivance, or . . . other manner" used to engaged in the prohibited conduct at issue here.

134. The Insight Tags operated on the Covered California Website and all of its subpages, and intercepted Plaintiff's and Class Members' sensitive health information communicated on Covered California's website and its subpages in real time.

135. Plaintiff and the Class members had a justified expectation under the circumstances that their electronic communications would not be intercepted.

136. LinkedIn had no right to intercept, collect, and disclose the Plaintiff's and the Class Members' sensitive health information. Neither Plaintiff nor the Class consented to LinkedIn's interception, disclosure, and/or use of their sensitive health information in their electronic communications with Covered California. Nor could they. LinkedIn never sought to or did obtain Plaintiff's or the Class Members' consent.

137. LinkedIn's conduct has needlessly harmed Plaintiff and the Class by disclosing intimately personal facts and data in the form of their sensitive health information. This disclosure and loss of privacy and confidentiality has caused the Plaintiff and the Class to experience mental anguish, emotional distress, worry, fear, and other harms.

138. Plaintiff and Class members seek all relief available relief under Cal. Penal Code § 631, including statutory damages of $2,500 per violation.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and all others similarly situated, asks for

judgment in their favor, and that the Court enter an order as follows:

A. Certifying the Class and appointing Plaintiff as the Class's representative;

B. Appointing Plaintiff's counsel as class counsel;

C. Finding that LinkedIn's conduct as alleged herein was unlawful;

D. Awarding such injunctive and other equitable relief as the Court deems just and proper, including enjoining LinkedIn from any further interception of Plaintiff or Class Members' communications to third parties without the Plaintiff or Class Members' express, informed, and written consent;

E. Awarding statutory damages to Plaintiff and Class Members pursuant to 18 U.S.C. § 2520 and Cal. Penal Code § 631;

F. Awarding damages for violations of Plaintiff and Class Members' right to privacy;

G. Awarding Plaintiff and Class Members statutory, actual, compensatory, consequential, punitive, and nominal damages, as well as restitution and/or disgorgement of profits unlawfully obtained;

H. Awarding Plaintiff and Class Members pre-judgment and post-judgment interest as provided by law;

I. Awarding Plaintiff and Class Members reasonable attorney's fees, costs, and expenses;

J. Awarding costs of suit; and

K. Such other and further relief to which Plaintiff and Class Members may be entitled.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all issues so triable.

Dated: May 15, 2025

LYNCH CARPENTER, LLP

By: */s/ (Eddie) Jae K. Kim*

(Eddie) Jae K. Kim (SBN 236805)
ekim@lcllp.com
Tiffine E. Malamphy (SBN 312239)
tiffine@lcllp.com
117 E Colorado Blvd, Ste 600
Pasadena, CA 91105-3712
Tel.: (213) 723-0707
Fax: (858) 313-1850

Nicholas A. Colella*
nickc@lcllp.com
Patrick D. Donathen*
patrick@lcllp.com
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
Tel: (412) 322-9243
Fax: (412) 231-0246

Attorneys for Plaintiff
and Proposed Class Counsel
* *Pro hac vice* forthcoming